Method and Apparatus for Creating a Message Digest Using a One-Way Hash Algorithm

Abstract of the Disclosure

A one-way hash algorithm is implemented in hardware and/or software. The hash algorithm creates a message digest from an input message. During one iteration of the hash algorithm, two or more "rounds" are performed, where a "round" is a calculation that operates on one word of a sequence of input words derived from the message, and each successive round operates on the next word in the sequence. The first round performed during each iteration includes at least one carry save adder (212, Figure 2) (CSA) and a full adder (224, Figure 2). The second round also includes at least one CSA (226, Figure 2) and a full adder (236, Figure 2). In one embodiment, the message digest computed by the hash algorithm is identical to a message digest computed using SHA-1, when given the same input message.

"Express Mail" mailing label number: EL721274905US
Date of Deposit: June 13, 2001
This paper or fee is being deposited on the date indicated above with the United States Postal Service pursuant to 37 CFR 1.10, and is addressed to BOX PATENT APPLICATION the Commissioner for Patents, Box Patent Application, Washington, D.C. 20231.